J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

사이버전 수행절차 운영개념에 관한 연구☆

A Study on the Operation Concept of Cyber Warfare Execution Procedures

김 성 중[1] 유 지 훈[1] 오 행 록[2] 신 동 일[1] 신 동 규[1*]
Sung-Joong Kim JiHoon Yoo HaengRok Oh Dongil Shin DongKyoo Shin

요 약

사이버공간의 확대로 인하여 전쟁양상 또한 재래전에서 사이버전을 포함한 형태로 바뀌어가고 있다. 사이버전이란 국가나 조직의 활동을 방해하기 위해 컴퓨터 기술을 사용하는 것으로 특히 국방 분야에서는 적 사이버 공격에 대해 체계적으로 대응할 필요성이 있다. 하지만 사이버 위협 환경에서 효과적으로 방어하기 위한 방어체계는 많이 미비하다. 이를 보완하기 위한 새로운 사이버전 운영 개념이 필요하다. 본 논문에서는 방어 중심의 사이버작전을 수행함에 있어 사이버작전 수행절차에 따라 요구되는 사이버 정보감시정찰, 능동적 방어 및 대응, 전투피해평가, 지휘통제 개념들을 효과적인 사이버작전 수행을 위해 통합적인 운용개념을 연구하고 이를 발전시켜 사이버전장에서 지속적인 전략적 우위를 달성할 수 있는 사이버전 운영 개념을 제시하고자 한다.

☞ 주제어 : 사이버전, 전투피해평가, 사이버 킬 체인

ABSTRACT

Due to the expansion of cyber space, war patterns are also changing from traditional warfare to cyber warfare. Cyber warfare is the use of computer technology to disrupt the activities of nations and organizations, especially in the defense sector. However, the defense against effective cyber threat environment is inadequate. To complement this, a new cyber warfare operation concept is needed. In this paper, we study the concepts of cyber intelligence surveillance reconnaissance, active defense and response, combat damage assessment, and command control in order to carry out cyber operations effectively. In addition, this paper proposes the concept of cyber warfare operation that can achieve a continuous strategic advantage in cyber battlefield.

☞ keyword : Cyber Warfare, Battle Damage Assessment

1. 서 론

정보통신과학기술의 발전으로 인터넷 사용량이 급증하고 현재는 스마트폰, 테블릿 PC 등 스마트 기기들의 출현으로 일상생활이 사이버공간으로 확대되는 변화를 가져오면서 삶의 질 또한 향상되었다. 하지만 이러한 변화들은 사이버전으로 대표되는 사이버공간에서의 전쟁 또한 만들어 냈다.

과거에는 물리적인 타격을 하는 재래전이었다면 현재는 사이버공간의 확대로 사이버 공격을 통해 전쟁 수행체계를 마비시키거나 파괴하는 전쟁환경의 변화를 가져왔다[1].

사이버전은 전략적 또는 군사적 목적을 위해 정보체계를 의도적으로 공격하는 것으로 사이버전의 위협은 지속적으로 발생 및 증가하고 있다. 2007년 에스토니아에서 발생한 대규모 사이버 공격 사건[2], 2010년 이란의 핵시설이 'Sturxnet'이라 불리는 웜 바이러스 공격[3] 등이 대표적인 사이버 공격 사건의 사례로 이러한 사례들은 사이버전이 현실화되었음을 확증해주는 근거가 되었다.

이러한 사이버 위협 환경에서 공격을 효과적으로 방어하기 위해서는 공격정보들을 신속하게 파악 및 식별하는 것이 중요하다. 그러나 기존의 사이버방어체계는 피해가 발생하면 복구를 하는데 중점을 두고 있다. 이를 보완하기 위해 새로운 사이버전 운영개념이 필요하다.

본 논문에서는 방어 중심의 사이버작전을 수행함에 있어 사이버작전 수행절차에 따라 요구되는 사이버 정보감시정찰, 능동적 방어 및 대응, 전투피해평가, 지휘통제 개념들을 효과적인 사이버작전 수행을 위해 통합적인 운용개념을 연구하고 이를 발전시켜 사이버전장에서 지속적

1 Department of Computer Engineering, Sejong University, Seoul, 05006, Korea
2 Agency for Defense Development
* Corresponding author (shindk@sejong.ac.kr)
[Received 14 November 2019, Reviewed 21 November 2019, Accepted 10 December 2019]
☆ 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다 (UD190016ED).

인 전략적 우위를 달성할 수 있는 사이버전 운영 개념을 제시하고자 한다.

2. 관련연구

이 섹션에서는 사이버전 프레임워크에 기초가 되는 사이버전과 Cyber Kill Chain에 대해서 설명한다.

2.1 사이버전

사이버전 프레임워크에 기반이 되는 개념인 사이버전은 Cyberwar와 많이 혼용해서 사용하는 개념으로 항상 많은 논쟁의 여지가 있는 개념이다[4]. 사이버전을 정의를 하려면, Cyberwarfare의 배경이 되는 Cyberspace에 대한 정의를 필요로 한다. Cyberspace는 디지털화된 정보가 컴퓨터 네트워크를 통해 전달되는 환경을 말하며, DoD (Department of Defense)에서는 정보 환경 내에서 글로벌 도메인으로 정의를 내렸다[5]. 글로벌 도메인은 인터넷, 통신 네트워크, 컴퓨터 시스템, 임베디드 프로세서 및 컨트롤러를 포함한 정보통신기술의 상호 의존적인 네트워크로 구성되며, 사이버 공간의 목표 달성을 위한 데이터 저장, 수정 및 교환하는데 사용된다. 위에서 정의된 Cyberspace에서 발생하는 사이버전에 대한 정의를 내리기 위해서 다양한 연구가 진행되었다. Hildreth와 Steven A는 사이버전에 대한 국가들의 관심이 높아지는 현상에 대한 문제를 제기했다[6]. 특히 사이버전의 사이버 공격과 관련해서 공격의 출처와 발생되는 피해를 평가하는 것에 대한 어려움을 얘기 했다. 이러한 문제에 대하여 대부분의 국가에서 사이버전을 군의 새로운 부분으로 통합하여 개발을 진행하고 있지만, 다수 국가들이 해당 문제3에 대해서 미국과 다른 견해를 가진다고 주장했다.

Jon R. Lindasy는 2010년 6월에 발생된 스턱스넷(Stuxnet) 사건을 통해, 사이버전의 영향이 경제와 문명을 파괴할 수 있을 정도로 국가에 가장 큰 위협이라 주장했다[7]. 이러한 사이버전을 방어하기 위해서 모든 군사 시스템이 통합되는 사이버 운영(Cyber Operation)을 제기하였으며, 사이버전이 단순하게 국가 및 군사 시스템뿐 아니라 민간 시스템들에도 관심을 가져야함을 강조했다.

Jeffrey Carr는 20~21세기에 발생한 국가별 다양한 사이버전 사례를 설명했다[8]. Cyberwarfare사례에 사용된 구체적인 구성요소들에 대해서 설명하였으며, 이를 전투 없는 전쟁으로 물리적 피해 없이 적에게 공격을 가하는 비물리적인 폭력행위라는 것을 강조했다.

Andrew Colarik는 기술의 발달로 인해 다양한 환경에서 정보를 수집, 보급 및 활용하는 현대 군사 작전에 대해서 설명한다[9]. 해당 연구에서는 군사 작전에도 통신 및 정보 인프라가 군의 최우선 목표로 변경되었으며, 실제 사이버 전쟁이 국가에 물리적인 피해를 입힐 수 있다는 점을 강조했다.

Lindasy는 스턱스넷(Stuxnet)을 사이버전에 대한 유일한 경험적 사례로 제시하며, 사이버전이 미치는 영향력에 대해서 설명했다[10]. 해당 연구에서는 사이버전의 막대한 영향력으로 인해 기존의 군사 및 정보 운영에 대한 보완으로 계속 발전 할 것이지만, 사이버 기기의 전략적 불확실성과 운영상의 복잡성으로 신뢰할 수 없는 전략적 도구가 될 것이라 주장한다.

2.2 사이버 킬 체인

Cyber Kill Chain은 군사적 개념인 "Kill Chain"을 사이버 공격 절차와 방어 개념에 적용한 것으로, 미 방위산업체 "록히드마틴(Rockheed Martin)"에 의해 정의되었다[11]. 여기서 사용되는 핵심 개념인 "Kill Chain"은 군사표적의 탐지부터 파괴까지의 과정을 탐지(Find), 식별(Fix), 추적(Track), 표적화(Target), 교전(Engage) 및 평가(Assess)로 구분된 단계를 말한다. Cyber Kill Chain은 이러한 "Kill Chain"의 개념을 이를 일련의 공격 및 방어 절차로 구성된 사이버전단계에 맞게 재구성한 모델이다. Cyber Kill Chain 모델은 방위산업체 및 국가별로 다양한 모델이 존재하며, 각각의 다른 단계의 모델로 구성된다. 다음은 Cyber Kill Chain의 가장 기본이 되는 록히드마틴에서 정의한 방어 절차 모델로 표 1과 같이 6단계로 구성된다.

(표 1) 록히드마틴 Cyber Kill Chain 방어 분류
(Table 1) Rockheed Martin Cyber Kill Chain defense classification

절차(단계)	내용
탐지	공격자의 행위정보를 발견
거부	공격자의 접근 및 사용을 차단
교란	공격을 위한 정보의 흐름 방해
약화	공격행위의 효율 또는 효과를 감소
기만	정보를 조작하여 공격자가 잘못된 판단 유도
파괴	공격자 또는 공격 관련 도구가 원래 기능을 수행하지 못하도록 손상 및 복구 불가능

(표 2) 록히드마틴 Cyber Kill Chain 공격 절차
(Table 2) Rockheed Martin Cyber Kill Chain Attack procedure

절차(단계)	내용
정찰	공격자가 목적을 달성하기 위해 공격 대상(표적)을 탐색, 식별 및 선정 단계
무기화	정찰단계에서 선정된 대상을 공격하기 위한 사이버 무기 준비 단계
유포	준비된 사이버 무기를 대상에게 퍼트리는 단계
악용	대상에게 전달된 사이버 무기의 악성코드가 활성화되는 단계
설치	공격자가 목표 시스템에 트로이 목마, 백도어등을 설치하여 목적 시스템에서 활동할 수 있는 환경을 조성하는 단계
명령 및 제어	공격자가 외부에서 목적 시스템을 통제할 수 있는 채널을 생성하는 단계
목적 달성	공격자가 의도한 목적을 달성하는 단계

표 2는 록히드마틴에서 정의한 공격 절차 모델로 다음과 같이 7가지로 분류했다. 위와 같이 록히드마틴에 의해 정의된 공격 및 방어 절차 개념을 대부분의 기업 및 국가들에서도 유사하게 사용한다.

“사이버안보 시험평가 가이드북”의 미 국방연구원(Institute for Defense Analysis)자료를 보면, 미 국방부에서는 공격과 방어의 주요 활동, 목적 등을 나타낸 “사이버안보킬체인(CSKC: Cybsersecurity Kill Chain) 자료를 볼 수 있다[12]. CSKC의 공격 절차는 록히드마틴의 7단계에서 설치 단계를 포함하지 않고 목적 달성 이후 유지하는 단계를 추가하였으며, 방어 절차의 경우 기존 록히드마틴의 방어 절차와 동일한 대응 유형을 사용한다.

가트너의 공격체인모델(Attack Chain Model)은 공격 절차를 전달, 악용 및 설치, 명령 및 제어, 권한 상승, 자원 접근, 탈취 6단계로 축약 하였다[13]. 축약된 공격 절차에서 정찰 및 무기화 단계를 포함시키지 않은 것과 다양한 공격 유형을 반영하기 위해 목적 달성 단계를 권한 상승, 자원 접근, 탈취 세분화한 점에서 록히드마틴 모델과 차이점이 있다.

휴렛패커드의 공격라이프사이클(AttackLifeCycle)은 공격 절차를 정찰, 공격 전달, 악용, 설치, 명령 및 제어, 지역적 탈취, 내부 탐색, 권한 상승, 채널 생성, 정보 탈취의 10단계로 구성했다[14]. 공격 절차에 무기화 단계를 포함하지 않고 공격자가 시스템에 침투한 이후 단계를 내부 탐색, 권한 상승, 정보 탈취 등으로 세분화한 것으로 록히드마틴 모델과 차별화되며, 가트너 모델과 유사함을 가진다.

국내에서는 록히드마틴의 Cyber Kill Chain 모델들이 이미 적이 네트워크 내부로 침입이 진행된 상태로, 방어자에게 수세적 대응만 할 수 있는 한계점에 대해서 지적하였고, 공세적 대응을 위한 사이버 Kill Chain 전략이 필요하다고 말하고 있다[15]. 해당 연구[15]에서는 표 3과 같이 4단계로 이루어진 국내의 “Kill Chain” 단계와 동일한 체계의 Cyber Kill Chain 모델을 맞추어 제안되었다.

(표 3) 제안된 국내 Cyber Kill Chain 체계
(Table 3) Proposed Inland Cyber Kill Chain

체계(단계)	내용
감시	공격자의 네트워크 혹은 체계를 감시할 수 있는 사이버 공간 감시 체계와 현실 세계의 감시체계를 통합한 감시체계
결심	Cyber Kill Chain 가동이후 추가적인 분쟁으로 확대되지 않기 위한 감시체계결과를 바탕으로 타격 근거를 제시할 수 있는 분석기술
타격	공격원점 타격, 지원세력 확대타격, 지휘세력 포함 타격으로 구성된 타격체계
연동	위의 3개의 체계(감시, 결심, 타격)이 별개가 아닌 유기적으로 작동하기 위한 운영 시스템

본 연구에서는 국내에서 제안된 Cyber Kill Chain 모델을 기반으로 방어자에게 수세적 대응하는 기존의 모델의 한계점을 극복할 수 있는 능동적 방어 기반의 사이버전 운영개념 프레임워크 구축방안을 제안한다.

3. 사이버전 운영개념 프레임워크 구축방안

최근 재래전 요소 및 사이버전 요소가 한 곳으로 수렴됨에 따라 통합작전에서는 지상 작전과 사이버작전의 통합이 필수적으로 요구되고 있다. 미 육군 사이버사령부에 따르면 사이버작전은 사이버공간을 통한 활동을 기획 및 동기화하여 기동의 자유를 도모하고 목표를 달성하는 행위를 의미하며 사이버공간에서의 작전은 사이버공간 정보·감시·정찰(Cyberspace ISR, Cyberspace Intelligence·Surveillance·Reconnaissance), 사이버공간 운용환경준비(Cyberspace OPE, Cyberspace Operational Preparation of the Environment), 방어적 사이버작전(DCO, Defensive Cyberspace Operations), 공세적 사이버공간 작전(OCO, Offensive Cyberspace Operations) 크게 4가지로 구성되며 각각의 활동은 사이버공간 활동 개념 하에 수행된다 [16]. 4가지의 활동을 살펴보면 사이버 정보·감시·정찰은 순사작전의

일환으로 수행하는 정보행위로, 작전부대 정보조직 및 임시 예속된 신호정보 조직을 활용한다. 그리고 작전적, 전술적 수준의 정보를 초점으로 군사작전 계획수립을 지원한다. 사이버공간 작전환경은 계획 또는 구상 중인 군사작전의 준비를 위한 여건조성을 목적으로 하며, 사이버공간에 대한 상황인식 및 의사결정을 수행한다. 사이버방어는 DoDIN을 운영, 보호, 방어하는 행위로 사이버 위협으로부터 탐지, 차단, 추적, 대응 등을 수행하며 사이버 방어활동을 실시한다. 마지막 사이버공격은 적의 정보, 정보시스템 및 네트워크를 변경 또는 통제하는 행위로 사이버공격 시 발생하는 피해를 예측하고 전투결과 확인을 수행한다.

본 논문에서 제안하는 사이버전 프레임워크는 이러한 4단계에서 착안하여 사이버 정보감시정찰, 사이버 지휘통제, 사이버방어, 사이버 전투피해평가로 구성하며 이 4단계를 유기적 관계로 구성한다.

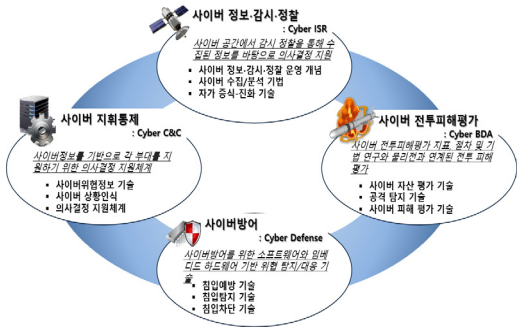
사이버공간 정보·감시·정찰은 사이버작전 및 대응을 지원하는데 필요한 목표대상 및 악의적인 공격자 또는 적의 시스템의 정보(Intelligence)를 능동적으로 수집하는 활동이다. 새로운 위협을 검색하고 모든 조치의 결과를 정보에기반하여 상황을 이해함으로써 사이버 지휘통제 의사결정에 정보를 제공한다. 적의 시스템 정보는 사이버 킬 체인(Cyber Kill Chain)을 기반한다.

사이버공간 운용환경준비는 사이버 정보·감시·정찰, 방어적 및 공세적 사이버 작전을 준비하고 지원하기 위한 활동으로 사이버 공격에 대비하기 위한 모든 운용활동을 총괄하고 정보 융합 및 공유를 수행한다.

방어적 사이버작전은 사이버 공간을 활용할 수 있는 능동적이고 수동적인 방법으로 사이버공간에서의 기동의 자유(Freedom of Manoeuvre)를 보장하며 정보보증 프레임워크 내에서 수행된다. 이는 능동적 방어(Active Defense), 수동적 방어(Passive Defense), 보안(Security), 탄력(Resilience)로 구성된다.

공세적 사이버공간 작전은 사이버 공간을 통하여 부인, 파괴 효과를 창출하는 행위를 의미한다. 이러한 행위는 사이버공간계층 개념에서 물리적 계층, 논리적 계층, 페르소나 계층 등 복합적으로 발생 가능하며 종합적인 보안 전략에서 공세적인 사이버 작전은 정보작전과의 협업과 사이버공간에서 발생하는 피해에 대하여 예측하는 행위가 필요하다.

본 논문에서 제안하는 사이버전 프레임워크 구축방안은 사이버공간 정보·감시·정찰, 사이버 지휘통제, 사이버방어, 소프트웨어와 임베디드 시스템 기반 하드웨어를 위

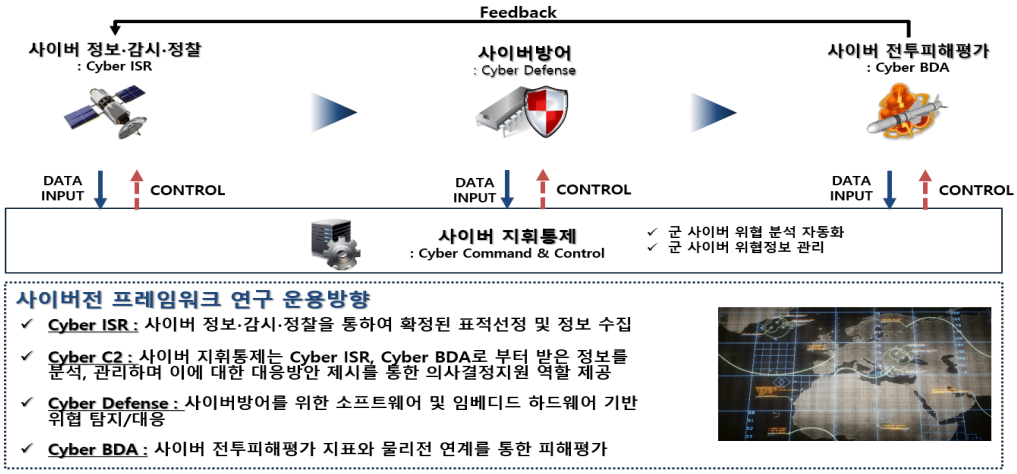


(그림 1) 사이버전 프레임워크 구축방안 개념
(Figure 1) Cyber warfare framework construction

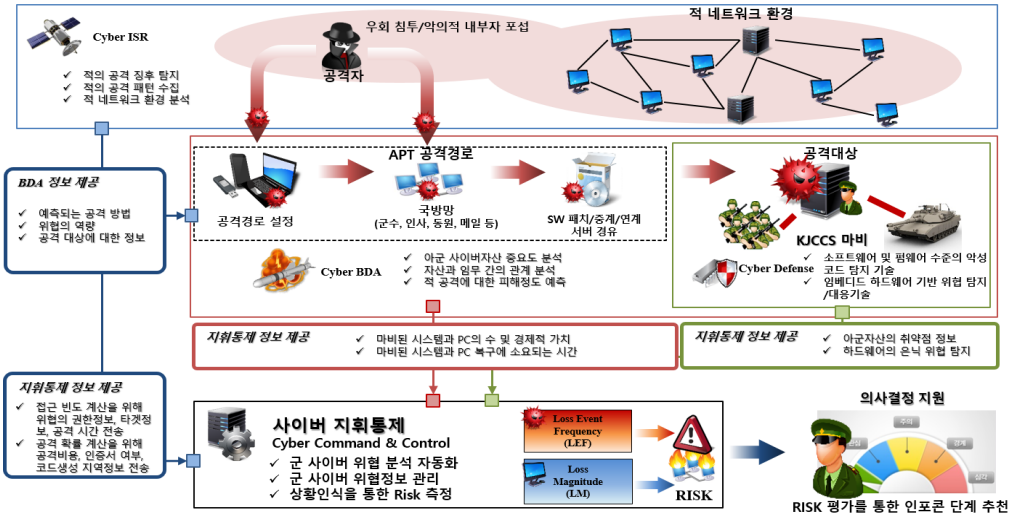
한 사이버보안 기술, 사이버 전투피해평가의 각 단계를 통하여 수집, 측정, 관리된 정보를 공유하는 프로세스를 가지며 이를 기반으로 사이버공간 작전체계의 통합 운용방안을 제시하고 더 나아가 사이버공간에서의 우위를 달성할 수 있는 사이버 지휘통제 운영개념을 제시하고자 한다.

그림 2는 사이버전 프레임워크 구축방안 통합 운용방안으로 사이버 정보·감시·정찰(Cyber ISR)에서 확정된 표적에 대한 정보·감시·정찰을 진행하며 수집된 정보를 사이버 지휘통제(Cyber C&C)의 사이버 위협정보 데이터베이스에 전달한다. 사이버방어에서는 능동적 방어를 기반으로 소프트웨어 기반 악성코드 탐지기술 및 위협/탐지기술, 펌웨어 수준의 악성코드 탐지 기술 및 임베디드 하드웨어 기반 위협 탐지/대응 기술을 연구하고 연구를 통해 수집된 취약점을 사이버 지휘통제의 사이버 위협정보 데이터베이스에 전달한다. 사이버 전투피해평가(Cyber BDA)는 사이버공간에 구성된 자산에 대하여 사이버 전투피해평가지표 및 사이버전과 물리전을 연계한 피해평가 방안을 개발하고 측정 및 예측한 지표를 사이버 지휘통제 프레임워크의 의사결정 지원체계에 전달한다. 사이버 지휘통제(Cyber C&C)는 각 단계에서 전달된 정보를 통합 운용 관리함으로써 사이버 상황인식에 기반한 의사결정 지원체계를 마련한다. 그리고 각 단계의 통합 운용개념을 구체화하기 위해 그림 3과 같이 APT공격을 기반으로 한 시나리오를 설정했다.

시나리오를 단계별로 보면 사이버 정보감시정찰 단계는 적 환경에 대한 정보수집이 필수이므로 사이버 위협을 발생시키는 적 또는 공격자의 공격 징후를 탐지하고, 적의 공격 패턴을 수집 및 적 네트워크 환경을 분석하여 이를 정보화하는 테스크를 부여했다. 사이버 전투피해평



(그림 2) 사이버전 프레임워크 구축방안 운용방안
(Figure 2) Cyber warfare framework operation plan



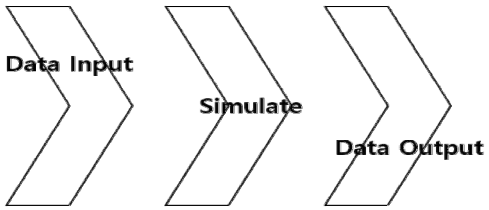
(그림 3) 사이버전 프레임워크 구축방안 시나리오
(Figure 3) Cyber warfare framework construction scenario

가 단계에서는 APT 공격경로와 공격 대상이 되는 아군 자산에 대한 분석을 담당한다. 아군 사이버 자산의 중요도 분석, 자산과 임무간의 관계분석, 적 공격에 대한 피해예측을 수행한다. 사이버방어 단계에서는 공격 대상이 되는 아군 자산에 대한 심도 있는 분석을 통하여 취약점 또는 악성행위를 탐지하는 행위를 수행한다. 마지막 사이버 지휘통제는 각 단계에서 수집, 분석된 정보와 자산 분석 데이터를 취합하여 risk를 도출하는 역할을 수행한다.

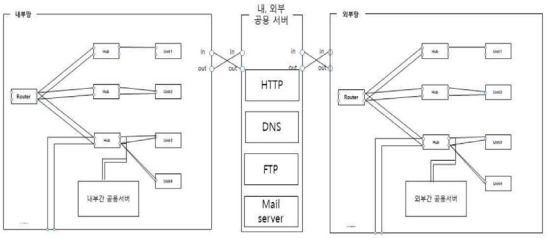
시나리오의 흐름을 보면 사이버 정보감시정찰은 사이버 전투피해평가에게 예측되는 공격방법, 위협정보 등 공격대상에 대한 정보를 전달하며, 사이버 지휘통제에게는 공격자의 접근 빈도와 같은 위협요소를 전달한다. 사이버 전투피해평가는 사이버 지휘통제에게 피해평가 결과내용을 전달한다. 이렇게 취합한 정보를 통하여 사이버 지휘통제에서 의사결정권자에게 도움을 줄 수 있는 정보를 제공한다.

4. 실 험

실험내용은 본 논문에서 제안한 사이버전 프레임워크 구축방안 4단계 중 사이버 전투피해평가에 대한 내용을 기술한다. 사이버전은 실제 물리전과 달리 피해를 직접적으로 식별할 수 없기 때문에 DEVSim++을 사용하여 사이버 피해평가를 위한 시뮬레이션을 진행했다. 시뮬레이션의 시나리오는 APT Stuxnet 공격 피해 시나리오이다. 시뮬레이션의 흐름은 그림 4와 같다.



(그림 4) 시뮬레이션 진행순서
(Figure 4) simulation procedure



(그림 5) 시뮬레이션 네트워크 구조
(Figure 5) simulation network architecture

초기 입력값은 다음과 같다. 시뮬레이션을 위해 가상으로 설정한 네트워크에 있는 unit, pc, server의 사이버 자산의 중요도, 사이버 자산의 수 등을 가지고 있는 파일을 입력한다. 그림 6은 시뮬레이터의 입력 데이터이다. 그리고 가상 네트워크 구조에 따라 사이버공격을 수행하는 시뮬레이션 과정을 진행한다. 공격이 종료되면 그림 8처럼 각 유닛마다 피해 받은 수치를 텍스트파일로 출력한다. 그림 5는 시뮬레이터의 가상 네트워크 구조이다.

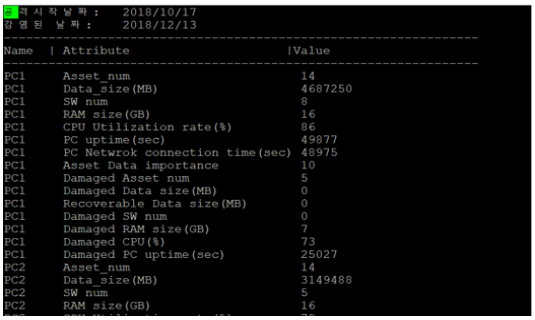
그리고 나서 공격 분류 기준으로 사용한 3가지 지표 Interruption, Interception, Modification을 MOCE(Measure Of Cyber Effectiveness)로 사용하여 피해율을 산출한다 [17]. 마지막으로 MOCE 최종 산출 이후에는 시각화하여 결과를 보여준다. 시각화는 그림 7과 같이 유닛 별로 Interruption, Interception, Modification의 피해율을 나타냈다. 그리고 pc와 서버의 피해율을 각각 표현했다. 시나리오 상 시스템 마비로 인한 Interruption 수치가 높은 것을 확인 할 수 있다.

Unit	Numerical value	mean
Whole PC num	10	전체 PC 수
Whole Asset num	100	전체 자산 수
Whole Data size(KB)	6924290048	전체 데이터 크기
Whole Software num	1931	전체 소프트웨어 수
Whole RAM size(GB)	192	전체 램 크기
Recuperator num	2	복구인원 수
Comm-Server		
Server bandwidth(Mhz)	15	서버 대역폭
Asset num	36	자산 수
Data size(KB)	1474297856	데이터 크기

(그림 6) 시뮬레이터 입력 값 예시
(Figure 6) simulator input data example

(그림 7) 피해평가 결과 시각화
(Figure 7) damage assessment visualization

직관적인 시각화를 통하여 사이버 지휘통제에서 판단의 지표로 사용하기가 편하여 의사결정권자에게 도움을 줄 수 있을 것으로 판단한다.



(그림 8) 시뮬레이션 결과
(Figure 8) simulation result

5. 결 론

본 논문에서는 사이버공간에서 사이버 작전을 수행함에 있어 요구되는 사항을 정보·감시·정찰, 지휘통제, 능동적 방어·공세적 대응, 전투피해평가로 구성한 사이버전 프레임워크를 구성하고, 이를 발전시켜 사이버전장에서 지속적인 전략적 우위를 달성할 수 있는 사이버전 운영개념을 제시했다. 그 중 전투피해평가 시뮬레이션 시스템을 설계 및 구현하고, 지휘통제 단계에서 지휘관의 결심을 돕기 위한 수단으로 피해평가 결과를 가시화했다.

향후 계획으로는 현재 제시한 사이버전 프레임워크를 발전시켜 추후 사이버작전을 위한 프레임워크를 제공하여 관련 기술과 작전운영절차 개발에 활용 가능할 것으로 보인다.

참고문헌(Reference)

[1] Park, Chan-soo and Park, Yongsuk, “A Study on the Improvement of Capability Assessment and the Plan for Enhancing Cyber Warfare Capability of Korea,” JKIICE vol. 19, no. 5, pp. 1251 - 1258, May 2015. https://doi.org/10.6109/jkiice.2015.19.5.1251

[2] Kaiser, R., “The Birth of Cyberwar,” Political Geography 46,pp.11~20, 2015. https://doi.org/10.1016/j.polgeo.2014.10.001

[3] James P. Farewell and Rafal Ronhozinski, “Stuxnet and the Future of Cyber War,” Survival 53, no.1, pp.23~40, February-March 2011. http://dx.doi.org/10.1080/00396338.2011.555586

[4] Robinson, M., Jones, K., & Janicke, H., ″Cyber warfare: Issues and challenges.″ Computers & security 49, pp.70-94, 2015. https://doi.org/10.1016/j.cose.2014.11.007

[5] Secretary of Defense. DoD Publications. http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf [accessed 17.08.10].

[6] Hildreth, Steven A. ″Cyberwarfare.″ LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2001.

[7] Lionel D. Alford Jr., “Cyber Warfare : A New Doctrine and Taxonomy,” The Journal of Defense Software Engineering 14, no.4, pp.27~30, April 2001.

[8] Jeffrey Carr, Inside Cyber Warfare 2nd edition, Sebastropol, CA : O’Reilly, 2012.

[9] Colarik, A., & Janczewski, L., “Establishing cyber warfare doctrine,” Current and Emerging Trends in Cyber Operations, pp. 37-50, Palgrave Macmillan, London, 2015. http://dx.doi.org/10.5038/1944-0472.5.1.3

[10] Lindsay, Jon R. ″Stuxnet and the limits of cyber warfare.″ Security Studies 22.3, pp.365-404, 2013. https://doi.org/10.1080/09636412.2013.816122

[11] Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. ″Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.″ Leading Issues in Information Warfare & Security Research 1.1, 80, 2011.

[12] Department of Defense, “Cybersecurity Test and Evaluation Guidebook. Version 2.0”, 2018.

[13] Ramon Krikken, Anton Chuvakin. “Selecting Security Monitoring Approaches by Using the Attack Chain Model,” Research ID G00264714. Gartner., 2014.

[14] Hewlett Packard Enterprise. “HPE Attack Life Cycle Use Case Methodology,” Technical White Paper, 2016.

[15] Yoo, Jae-won, and Dea-woo Park. ″Cyber kill chain strategy for hitting attacker origin.″ Journal of the Korea Institute of Information and Communication Engineering 21.11, 2199-2205, 2017. https://doi.org/10.6109/jkiice.2017.21.11.2199

[16] Department of Defense, “ARCYBER The NEXT Battlefield”, 2013.12.10.

[17] Park, JinHo, et al. ″Design and Implementation of Simulation Tool for Cyber Battle Damage Assessment Using MOCE (Measure of Cyber Effectiveness).″ Journal of the Korea Institute of Information Security and Cryptology, 29.2, 465-472, 2019. https://doi.org/10.13089/JKIISC.2019.29.2.465

◐ 저 자 소 개 ◑

김 성 중(sungjoong Kim)
2016년 서울호서직업전문학교 사이버해킹보안과 졸업
2018년 세종대학교 컴퓨터공학과 석사
2019년~현재 세종대학교 컴퓨터 공학과 박사 과정
관심분야 : 정보보호, 사이버전, 데이터마이닝
E-mail : tjdwnd2004@sju.ac.kr

유 지 훈(Jihoon Yoo)
2016년 서울호서직업전문학교 사이버해킹보안과 졸업
2018년 세종대학교 컴퓨터공학과 석사
2019년~현재 세종대학교 컴퓨터 공학과 박사 과정
관심분야 : 정보보호, 데이터마이닝, 머신러닝
E-mail : yoojihoon@sju.ac.kr

오 행 록(HaengRok Oh)
1987년 인하대학교 전산학과(학사)
1989년 인하대학교 전산학과(석사)
2004년 고려대학교 컴퓨터학과(박사수료)
1989년~현재 국방과학연구소 수석연구원
관심분야 : 사이버보안, 사이버 지휘통제
E-mail : haengrok@add.re.kr

신 동 일(Hyukjin Kwon)
1988년 연세대학교 컴퓨터과학과 졸업
1993년 Washington State University 컴퓨터과학과 석사
1997년 North Texas University 컴퓨터과학과 박사
1998년~현재 세종대학교 컴퓨터공학과 교수
관심분야 : 정보보호, 생체신호 데이터처리, 데이터마이닝, 머신러닝
E-mail : dshin@sejong.ac.kr

신 동 규(Dongkyoo Shin)9pt
1986년 서울대학교 계산통계학과 졸업
1992년 Illinois Institute of Technology 컴퓨터과학과 석사
1997년 Texas A&M University 컴퓨터과학과 박사
1998년~현재 세종대학교 컴퓨터공학과 정교수
관심분야 : 정보보호 , 사이버전, 머신러닝, u-헬스케어
E-mail : shindk@sejong.ac.kr